UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

IN RE: BETMGM DATA BREACH LITIGATION	Civil Action No. 22-7462 (JXN) (CLW)
	CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiff Scott Madlinger ("Plaintiff"), individually and on behalf of all others similarly situated ("Class Members"), alleges upon personal knowledge as to his own actions and his Counsel's investigation, and upon information and behalf as to all others matters, states as follows:

INTRODUCTION

1. Plaintiff brings this Class Action Complaint ("Complaint") against Defendant BetMGM, LLC ("Defendant" and/or "BetMGM") for its failure to properly secure and safeguard personally identifiable information ("PII")[1] for past and current customers of Defendant, including, but not limited to their names, mailing addresses, telephone numbers, email addresses, dates of birth, portions of their Social Security Numbers, and BetMGM identifiers including player ID and screen names.

2. According to its website, Defendant was created as a partnership between MGM Resorts International and Entain Holdings intending to access the sports betting and online gaming market in the United States. Defendant is based in Jersey City, New Jersey.[2]

3. BetMGM is now one of the world's largest sports betting and igaming operators,

[1] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual.

[2] *What We Do*, BetMGM, available at: https://www.betmgminc.com/what-we-do/ (last visited December 21, 2022).

with revenues in 2021 over $850 Million in 2021.[3]

4. As a regular and necessary part of its business, Defendant acquires and stores vast amounts of sensitive and non-public consumer data.

5. Prior to and through May 2022, Defendant obtained the PII of Plaintiff and Class Members, and stored that PII, unencrypted, in an Internet-accessible environment on Defendant's network.

6. Defendant understands the need to safeguard the PII that it collects and maintains for its pecuniary benefit. Defendant's Privacy Policy (the "Privacy Policy"), posted on its website, represents that:

> BetMGM is committed to protecting the security of your Personal Data. We maintain commercially reasonable safeguards to maintain the security and privacy of Personal Data that we collect and use in connection with our Operations. Nevertheless, when disclosing Personal Data, you should remain mindful that there is an inherent risk in the use of email and the internet. Your information may be intercepted without our knowledge or consent, collected illegally and/or used by third parties that are not affiliated with and/or controlled by us without your consent. We cannot guarantee the security of any information you disclose online, and you do so at your own risk.[4]

7. Despite this, on November 28, 2022, Defendant learned of a data security incident on its network and determined that an unknown actor compromised and accessed the PII of Defendant's past and current customers, including Plaintiff and Class Members (the "Data Breach").

8. Defendant is under the belief that the Data Breach occurred in May 2022, based on admissions in its Notice of Data Breach ("Notice Letter") sent to the Plaintiff and Class members

[3] Conor Porter, *BetMGM Expects To Exceed $1.3bn In 2022 Net Revenue*, SBCAmericas (Jan. 19, 2022), available at: https://sbcamericas.com/2022/01/19/betmgm-expects-to-exceed-1-3bn-in-2022-net-revenue/ (last visited April 11, 2023).

[4] Privacy Policy, BetMGM, available at: https://www.betmgminc.com/privacy-policy/ (last visited Dec. 13, 2022).

on December 21, 2022.

9. By obtaining, maintaining, collecting, using, and deriving a benefit from the PII of Plaintiff and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion. In its Notice Letter, Defendant stated that an unauthorized actor unlawfully acquired unencrypted PII including names, mailing addresses, telephone numbers, email addresses, dates of birth, portions of their Social Security Numbers, and BetMGM identifiers such as player ID and screen names.

10. The exposed PII of Plaintiff and members of the Class and Subclass will likely be sold on the dark web. Hackers target companies like Defendant to access and then offer for sale the unencrypted, unredacted PII they maintain to other criminals. Plaintiff and members of the Class and Subclass now face a lifetime risk of identity theft, which is heightened here by the loss of portions of their Social Security Numbers in conjunction with verifying information like the names and dates of birth of Plaintiff and Plaintiff and members of the Class and Subclass.

11. The PII was compromised due to Defendant's negligent and/or careless acts and omissions regarding the condition of its data security practices and the failure to protect the PII of Plaintiff and members of the Class and Subclass.

12. As a result of this delayed response, Plaintiff and members of the Class and Subclass had no idea their PII had been compromised and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm, including the sharing and detrimental use of their sensitive information. This risk will remain for their respective lifetimes.

13. Plaintiff brings this action on behalf of all persons whose PII was compromised as a result of Defendant's failure to: (i) adequately protect the PII of Plaintiff and members of the

Class and Subclass; (ii) warn Plaintiff and members of the Class and Subclass of Defendant's inadequate information security practices; (iii) effectively secure hardware containing protected PII using reasonable and adequate security procedures free of vulnerabilities and incidents; and (iv) timely notify Plaintiff and members of the Class and Subclass of the Data Breach. Defendant's conduct amounts at least to negligence and violates federal and state statutes.

14. Plaintiff and members of the Class and Subclass have suffered injury as a result of Defendant's conduct. These injuries include: (i) lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time, (iv) the disclosure of their private information, and (v) the present, continued, and certainly increased risk to their PII, which remains unencrypted and available for unauthorized third parties to access and abuse; and may remain backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

15. Defendant disregarded the rights of Plaintiff and members of the Class and Subclass by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that the PII of Plaintiff and members of the Class and Subclass was safeguarded, failing to take available steps to prevent unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols concerning data security and failing to enact policies and procedures regarding the encryption of data, even for internal use. As a result, the PII of Plaintiff and Class and Subclass members was compromised through disclosure to an unauthorized third party. Plaintiff and members of the Class and Subclass have a continuing

interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

PARTIES

16. Plaintiff Scott Madlinger resides in Toms River, New Jersey, and is a citizen of New Jersey.

17. Defendant BetMGM is a limited liability company registered in the State of New Jersey with a principal place of business in Jersey City, New Jersey.

18. The true names and capacities of persons or entities, whether individual, corporate, associate or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiff. Plaintiff will seek leave of court to amend this complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

19. All of Plaintiff's claims stated herein are asserted against Defendant and any of its owners, predecessors, successors, subsidiaries, agents, and/or assigns.

JURISDICTION AND VENUE

20. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed classes, and at least one Class or Subclass Member is a citizen of a state different from Defendant to establish minimal diversity.

21. Defendant is a citizen of New Jersey because it is a corporation formed under New Jersey law, and its principal place of business is in Jersey City, New Jersey.

22. The District of New Jersey has personal jurisdiction over Defendant because it conducts substantial business in New Jersey and this District.

23. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendant operates in this District, and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District.

FACTUAL ALLEGATIONS

Background

24. Plaintiff and members of the Class and Subclass are past and current customers of Defendant, who provided, entrusted, or allowed Defendant to maintain their sensitive and confidential information, including their names, dates of birth, and driver's license numbers or state identification numbers.

25. Plaintiff and members of the Class and Subclass value the integrity of their PII and demand reasonable security to safeguard their PII. Plaintiff and members of the Class and Subclass relied on the sophistication of Defendant, an industry leading company, to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

26. As a result of collecting and storing the PII of Plaintiff and members of the Class and Subclass for its own pecuniary benefit, Defendant had a duty to adopt reasonable measures to protect the PII of Plaintiff and members of the Class and Subclass from involuntary disclosure to third parties.

The Data Breach

27. On or about December 21, 2022, Defendant sent Plaintiff and members of the Class and Subclass a letter titled *Important Notice About Your Personal Information* (the "Notice"). Defendant's Notice, in pertinent part, informed Plaintiff and other Class Members:

What Happened?

Dear Patron,

We are writing to notify you of an issue that involves certain of your personal information. We have learned that certain BetMGM patron records were obtained in an unauthorized manner. We believe that your information was contained in these records, which may have included details such as name, contact information (such as postal address, email address and telephone number), date of birth, hashed Social Security number, account identifiers (such as player ID and screen name) and information related to your transactions with us. The affected information varied by patron.

We promptly launched an investigation after learning of the matter and have been working with leading security experts to determine the nature and scope of the issue. We learned of the issue on November 28, 2022, and believe the issue occurred in May 2022. We currently have no evidence that patron passwords or account funds were accessed in connection with this issue. Our online operations were not compromised. We are coordinating with law enforcement and taking steps to further enhance our security.

We recommend you remain alert for any unsolicited communications regarding your personal information and review your accounts for suspicious activity. We take our obligation to safeguard personal information very seriously and have arranged to offer you credit monitoring and identity restoration services for two years at no cost to you. The Reference Guide below provides instructions on enrolling in these services and steps you can take to protect your information.

28. Defendant stated in its Notice Letter that an unauthorized actor accessed sensitive information about Plaintiff and members of the Class and Subclass, including their names, mailing addresses, telephone numbers, email addresses, dates of birth, portions of their Social Security Numbers, and BetMGM identifiers including player ID and screen names.

29. In response to the Data Breach, Defendant claimed that "We are coordinating with law enforcement and taking steps to further enhance our security." The details of those safeguards and the remedial measures undertaken, have not been shared with regulators or Plaintiff and

members of the Class and Subclass, who retain a vested interest in ensuring that their information remains protected.

30. The unencrypted PII of Plaintiff and members of the Class and Subclass will likely end up for sale on the dark web, or fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiff and members of the Class and Subclass. As a result of the Data Breach, unauthorized individuals can easily access the PII of Plaintiff and members of the Class and Subclass. Indeed, as detailed below, the exposed PII of Plaintiff, and members of the Class and Subclass, has already been misused as a result of the Data Breach.

31. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it maintained for Plaintiff and members of the Class and Subclass, causing the exposure of PII for Plaintiff and members of the Class and Subclass.

32. Because Defendant had a duty to protect the PII of Plaintiff and members of the Class and Subclass, Defendant should have accessed readily available and accessible information about potential threats for the unauthorized exfiltration and misuse of such information.

33. As evidenced by Defendant's Privacy Policy and public statements regarding data security, Defendant knew or should have known that (i) cybercriminals were targeting large companies such as Defendant's, (ii) cybercriminals were ferociously aggressive in their pursuit of large companies such as Defendant's, and (iii) cybercriminals were publishing stolen PII on dark web portals.

34. In light of information readily available and accessible on the internet before the Data Breach, Defendant, having elected to store the unencrypted PII of Plaintiff and members of the Class and Subclass in an Internet-accessible environment, had reason to be on guard for the

exfiltration of PII and knew that due to its public profile, Defendant had cause to be particularly on guard against such an attack.

35. Prior to the Data Breach, Defendant knew and understood the foreseeable risk that Plaintiff and members of the Class and Subclass' PII could be targeted, accessed, exfiltrated, and published as the result of a cyberattack.

36. Prior to the Data Breach, Defendant knew or should have known that it should have encrypted the driver's license numbers and other sensitive data elements within the PII it maintained to protect against its publication and misuse in the event of a cyberattack.

37. Prior to the Data Breach, Defendant knew or should have known that it should not store sensitive and confidential information in an internet accessible environment without the necessary encryption, detection, and other basic data security precautions that would have prevented this Data Breach.

Defendant Acquires, Collects, and Stores the PII of Plaintiff and Class Members.

38. As a condition of receiving services from Defendant, Defendant required that its customers entrust Defendant with highly confidential PII. Plaintiff and members of the Class and Subclass provided their PII on the condition and with the expectation that it be maintained as confidential and safeguarded against unauthorized access.[5]

39. Defendant acquired, collected, and stored the PII of Plaintiff and members of the Class and Subclass and used it to derive a substantial portion of its revenue.

[5] Plaintiff provided his PII to Borgata in 2013, and BetMGM succeeded to the rights and obligations to maintain the confidentiality of Plaintiff's PII by virtue of its acquisition of Borgata's online betting business in 2016. *See* *https://investors.mgmresorts.com/investors/news-releases/press-release-details/2016/MGM-Growth-Properties-LLC-and-MGM-Resorts-International-Complete-Transactions-for-Acquisition-of-Borgata-Hotel-Casino--Spa/default.aspx* (last accessed April 14, 2023).

40. By obtaining, collecting, and storing the PII of Plaintiff and members of the Class and Subclass, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting the PII from disclosure.

41. Plaintiff and members of the Class and Subclass have taken reasonable steps to maintain the confidentiality of their PII and relied on Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

Securing PII and Preventing Breaches

42. Defendant's negligence in safeguarding the PII of Plaintiff and members of the Class and Subclass is especially egregious as the frequency and danger of data breaches are well known. Large companies, such as Defendant's, have received multiple warnings and alerts directed at protecting and securing sensitive data.

43. In light of recent high profile data breaches at other industry leading companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendant knew or should have known that cybercriminals would target its electronic records.

44. Indeed, cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets. Thus, they are aware of, and prepared for, a potential attack.

45. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII of Plaintiff and members

of the Class and Subclass from being compromised.

46. Defendant could have prevented this Data Breach by properly securing and encrypting the folders, files, and/or data fields containing the PII of Plaintiff and members of the Class and Subclass. Alternatively, Defendant should have destroyed the data it no longer had a reasonable need to maintain or only stored data in an Internet-accessible environment when there was a reasonable need to do so and with proper safeguards.

47. Several best practices have been identified that at a minimum should be implemented by Defendant, including but not limited to employing: strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; and limiting access to sensitive data.

48. Other best cybersecurity practices include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; protecting against any possible communication system; and training staff regarding critical points; and increasing the frequency of Penetration Testing.

49. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

50. These foregoing frameworks are existing and applicable industry standards..

Defendant failed to comply with these accepted standards, opening the door to cybercriminals and causing the Data Breach.

51. Federal and State governments have likewise established security standards and issued recommendations to temper data breaches and harm to consumers and financial institutions. The Federal Trade Commission ("FTC") has issued numerous guides for businesses highlighting the importance of reasonable data security practices. According to the FTC, data security should be factored into all business decision-making.[6]

52. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[7] The guidelines note that businesses should protect the personal consumer and consumer information they keep, properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems.

53. The FTC recommends that companies verify that third-party service providers have implemented reasonable security measures.[8]

54. The FTC recommends that businesses:

a. Identify all connections to the computers where you store sensitive information;

b. Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks;

c. Do not store sensitive consumer data on any computer with an internet

[6] Federal Trade Commission, *Start With Security*, *available at*: https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.
[7] Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, *available at*: https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business.
[8] FTC, *Start With Security*, *supra* note 5.

connection unless it is essential for conducting their business;

d. Scan computers on their network to identify and profile the operating system and open network services - Services that are not needed should be disabled to prevent hacks or other potential security problems. For example, if an email service or an internet connection is not necessary on a certain computer, a business should consider closing the ports to those services on that computer to prevent unauthorized access to that machine;

e. Pay particular attention to the security of their web applications—the software used to give information to visitors to their websites and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hack attacks;

f. Use a firewall to protect their computers from hacker attacks while connected to a network, especially the internet;

g. Determine whether a border firewall should be installed where the business's network connects to the internet - A border firewall separates the network from the internet and may prevent an attacker from accessing a computer on the network where sensitive information is stored. Set access controls—settings that determine which devices and traffic get through the firewall—to allow only trusted devices with a legitimate business need to access the network. Since a firewall's protection is only as effective as its access controls, they should be reviewed periodically;

h. Monitor incoming traffic for signs that someone is trying to hack in - Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day; and

i. Monitor outgoing traffic for signs of a data breach - Watch for unexpectedly large amounts of data being transmitted from their system to an unknown user. If large amounts of information are being transmitted from a business network, the transmission should be investigated to make sure it is authorized.

55. The FTC has brought enforcement actions against businesses for failing to protect consumer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an

unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45 *et seq*.

56. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

57. Defendant was at all times fully aware of its obligation to protect employees' personal and financial data, including Plaintiff and members of the Class and Subclass. Defendant was also aware of the significant repercussions if it failed to do so.

58. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data, including the PII of Plaintiff and members of the Class and Subclass, constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45 *et seq*.

59. The ramifications of Defendant's failure to secure the PII of Plaintiff and members of the Class and Subclass are long lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

Value of Personal Identifiable Information

60. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[9] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification

[9] 17 C.F.R. § 248.201 (2013).

number."[10]

61. The PII of individuals is of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, PII can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[11] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[12]

62. Plaintiff and members of the Class and Subclass' PII is of great value to hackers and cybercriminals, and the data stolen in the Data Breach has been used and will continue to be used in a variety of sordid ways for criminals to exploit Plaintiff and members of the Class and Subclass and to profit off their misfortune.

63. Identity thieves use personal information for various crimes, including credit card fraud, phone or utility fraud, and bank/finance fraud.[13] According to Experian, one of the largest credit reporting companies in the world, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to among other things: open a new credit card or loan, change a billing address so the victim no longer receives bills, open new utilities, obtain a mobile phone, open a bank account and write bad checks, use a debit card

---

[10] *Id*.

[11] Anita George, *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed Dec. 21, 2022).

[12] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed Dec. 21, 2022).

[13] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 12 C.F.R. § 1022.3(h). The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 12 C.F.R. § 1022.3(g).

number to withdraw funds, obtain a new driver's license or ID, and/or use the victim's information in the event of arrest or court action.[14]

64. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity -- or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

65. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through spam phone calls and text messages or phishing emails. Data Breaches can be the starting point for these other targeted attacks on the victims.

66. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States.[15] For example, the driver's license and state issued identification information stolen in the Data Breach can be used to create fake driver's licenses, open accounts in your name, avoid traffic tickets or collect government benefits such as unemployment checks.[16] These criminal

---

[14] Susan Henson, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself?* Experian, Sept. 1, 2017, *available at*: https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/ (last visited December 21, 2022).

[15] *Facts + Statistics: Identity Theft and Cybercrime*, Insurance Info. Inst., *available at*: https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (last visited April 11, 2023).

[16] Gayle Sato, *What Should I Do if My Driver's License Number is Stolen*? Experian, *available at*: https://www.experian.com/blogs/ask-experian/what-should-i-do-if-my-drivers-license-number-is-stolen/ (last visited December 21, 2022).

activities have and will result in devastating financial and personal losses to Plaintiff and members of the Class and Subclass.

67. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of organization-specific information such as retailer credit card information. For example, credit card information stolen from a retailer can be less valuable as victims can cancel or close credit and debit card accounts, thus preventing future fraud from occurring. On the other hand, the information compromised in this Data Breach is much more difficult to "close" if not impossible, to change.

68. This was a financially motivated Data Breach, as the only reason the cybercriminals go through the trouble of running a targeted cyberattack against a company like BetMGM is to get information that they can monetize by selling on the black market for use in the kinds of criminal activity described herein. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, [PII] and Social Security Numbers are worth more than 10x on the black market." [17]

69. PII is such a valuable commodity to identity thieves that once it has been compromised, criminals will use it and trade the information on the cyber black-market for years.[18] For example, it is believed that identity thieves used certain highly sensitive personal information compromised in the 2017 Experian data breach three years later to apply for COVID-19-related unemployment benefits.

---

[17] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Dec. 21, 2022).

[18] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO, July 5, 2007, https://www.gao.gov/products/gao-07-737 (last visited December 21, 2022)

70. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[19]

71. Identity theft is a challenging problem to solve. In a survey, the Identity Theft Resource Center found that most victims of identity crimes need more than a month to resolve issues stemming from identity theft and some need over a year.[20] Victims of the Data Breach, like Plaintiff and Class and Subclass members, must spend many hours and large amounts of money protecting themselves from the current and future adverse impacts to their credit because of the Data Breach.[21]

72. As a direct and proximate result of the Data Breach, Plaintiff and members of the Class and Subclass suffer from an imminent, immediate, and continuing increased risk of harm from fraud and identity theft. Plaintiff and members of the Class and Subclass must now take the time and effort and spend the money to mitigate the actual and potential impact of the Data Breach on their everyday lives, such as: (1) including purchasing identity theft and credit monitoring services; (2) placing "freezes" and "alerts" with credit reporting agencies; (3) contacting their financial institutions; (4) closing or modifying financial accounts, and (5) closely reviewing and monitoring bank accounts, credit reports, and other related activity for unauthorized activity for

---

[19] *Id*.
[20] *2021 Consumer Aftermath Report: How Identity Crimes Impact Victims, their Families, Friends, and Workplaces*, Identity Theft Resource Center (2021), available at: https://www.idtheftcenter.org/identity-theft-aftermath-study/ (last visited December 21, 2022).
[21] *Guide for Assisting Identity Theft Victims*, Federal Trade Commission, 4 (Sept. 2013) available at, http://www.global-screeningsolutions.com/Guide-for-Assisting-ID-Theft-Victims.pdf. (last visited December 21, 2022)

years to come.

73. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and members of the Class and Subclass, including driver's license numbers, and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and members of the Class and Subclass as a result of a breach.

74. Plaintiff and Class and Subclass members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. Plaintiff and members of the Class and Subclass will continue to incur such damages in addition to any fraudulent use of their PII.

75. Defendant was, or should have been, fully aware of the unique type and the significant volume of data contained in Defendant's database, amounting to potentially millions of individuals. Defendant should have known of the risk to the significant number of individuals whom the exposure of the unencrypted data would harm.

76. To date, Defendant has offered Plaintiff and members of the Class and Subclass only one year of credit monitoring and identity theft detection through Equifax. The offered service is inadequate to protect Plaintiff and members of the Class and Subclass from the threats they face for years to come, particularly in light of the PII at issue here.

77. Plaintiff and members of the Class and Subclass have suffered, and continue to suffer, actual harms for which they are entitled to compensation, including for:

a. Trespass, damage to, and theft of their personal property including Personal Information;

b. Improper disclosure of their Personal Information;

c. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their Personal Information being placed in the hands of criminals and having been already misused;

d. The imminent and certainly impending risk of having their Personal Information used against them by spam callers to defraud them;

e. Damages flowing from Defendant's untimely and inadequate notification of the data breach;

f. Loss of privacy suffered as a result of the Data Breach;

g. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the data breach;

h. Ascertainable losses in the form of deprivation of the value of customers' personal information for which there is a well-established and quantifiable national and international market;

i. The loss of use of and access to their credit, accounts, and/or funds;

j. Damage to their credit due to fraudulent use of their Personal Information; and

k. Increased cost of borrowing, insurance, deposits and other items that are adversely affected by a reduced credit score.

78. Moreover, Plaintiff and members of the Class and Subclass have an interest in ensuring that their information, which remains in possession of Defendant, is protected from further breaches by the implementation of industry standards and statutorily compliant security measures and safeguards. Defendant has shown itself incapable of protecting Plaintiff's and Class members' PII.

79. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class Members.

Plaintiff Madlinger's Experience

80. Plaintiff Madlinger provided his PII to Borgata sometime in 2013 when he visited

Borgata's website and signed up for an account.[22] At that time, Plaintiff provided his name, address, date of birth, social security number, and certain financial information to Borgata. BetMGM eventually came into possession of Madlinger's PII.

81. Plaintiff and members of the Class and Subclass entrusted their PII to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access. Plaintiff Madlinger would not have allowed BetMGM to maintain his PII if he believed Defendant would fail to safeguard that information from unauthorized access.

82. Plaintiff received an email from Defendant, dated December 21, 2022, informing him that his PII, including his name, mailing address, telephone number, email address, date of birth, portions of his Social Security Number, and BetMGM account identifiers including player ID and screen name, was identified as having been accessed by cybercriminals during the Data Breach.

83. Because of the Data Breach, Plaintiff's Private Information is now in the hands of cybercriminals. Plaintiff and all Class and Subclass members are imminently at risk of future identity theft and fraud.

84. As a result of the Data Breach, Plaintiff has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach. Specifically, Plaintiff has devoted time to, among other things, investigating the Data Breach, researching how best to ensure that he is protected from identity theft, dealing with an increase in spam phone calls and emails, and reviewing account

[22] Borgata is an indirect wholly owned subsidiary of MGM Resorts International ("MGM"). MGM is one of the co-owners of BetMGM.

statements and updating passwords.

85. Plaintiff Madlinger anticipates spending additional time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Madlinger will continue to be at present, imminent, and continued increased risk of identity theft and fraud for years to come.

86. Plaintiff has suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's PII; (b) identity theft and data misuse in the form of fraudulent charges and a notification that his information has been posted on the dark web; (c) the imminent and certain impending injury flowing from fraud and identity theft posed by Plaintiff's PII being placed in the hands of cyber criminals; (d) damages to and diminution in value of Plaintiff's Private Information that was entrusted to Defendant with the understanding that Defendant would safeguard this information against disclosure; (e) loss of the benefit of the bargain with Defendant to provide adequate and reasonable data security—*i.e.*, the difference in value between what Plaintiff should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security and failing to protect Plaintiff's PII; and (f) continued risk to Plaintiff's PII, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the PII that was entrusted to Defendant.

V. CLASS ALLEGATIONS

87. Plaintiff brings this nationwide class action on behalf of themselves and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

88. The Rule 23(b)(2) Nationwide Class (the "Class") that Plaintiff seeks to represent

is defined as follows:

> All individuals whose PII was compromised in the data breach subject to the *Notice of Recent Security Incident* that Defendant sent to Plaintiff and Class Members on or around December 21, 2022 (the "Nationwide Class").

89. The Rule 23(b)(3) Nationwide Subclass (the "Subclass" that Plaintiff seeks to represent is defined as follows:

> All members of the Nationwide Class whose agreements with BetMGM do not contain an arbitration clause.

90. Excluded from the Class and Subclass are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

91. Plaintiff reserves the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

92. Numerosity, Fed R. Civ. P. 23(a)(1): The Class and Subclass are so numerous that the joinder of all members is impracticable. Defendant has identified numerous individuals whose PII was compromised in the Data Breach, and the Class and Subclass Members are readily identifiable within Defendant's records.

93. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): There are questions of law and fact common to the Class and Subclass Members. These include:

a. Whether and to what extent Defendant had a duty to protect the PII of Class and Subclass Members;

b. Whether Defendant had duties not to disclose the PII of Class and Subclass Members to unauthorized third parties;

c. Whether Defendant had duties not to use the PII of Class and Subclass Members for non-business purposes;

d. Whether Defendant failed to adequately safeguard the PII of Class and Subclass Members;

e. When Defendant learned of the Data Breach;

f. Whether Defendant adequately, promptly, and accurately informed Class and Subclass Members that their PII had been compromised;

g. Whether Defendant violated the law by failing to promptly notify Class and Subclass Members that their PII had been compromised;

h. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Class and Subclass Members;

k. Whether Class and Subclass Members are entitled to actual, consequential, and/or nominal damages as a result of Defendant's wrongful conduct;

l. Whether Class and Subclass Members are entitled to restitution as a result of Defendant's wrongful conduct; and

m. Whether Class and Subclass Members are entitled to injunctive relief to redress the imminent and currently ongoing harm from the Data Breach.

94. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiff's claims are typical of those of other Class and Subclass Members because all had their PII compromised as a result of the Data Breach, due to Defendant's misfeasance.

95. Predominance: The common questions of law and fact predominate over any questions affecting only individual Subclass Members.

96. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

97. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiff will fairly and adequately represent and protect the interests of the Class and Subclass Members in that they have no disabling conflicts of interest that would be antagonistic to those of the other Class and Subclass Members. Plaintiff seeks no relief that is antagonistic or adverse to the Class and Subclass Members and the infringement of the rights and the damages they have suffered are typical of other Class and Subclass Members. Plaintiff has retained counsel experienced in complex class action litigation and intends to prosecute this action vigorously.

98. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): The class litigation is an appropriate method for fair and efficient adjudication of the Subclass claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Subclass Members to prosecute their common claims in a single forum simultaneously, efficiently, and without unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Subclass Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Subclass Members who could afford to litigate such a claim, it

would still be economically impractical and impose a burden on the courts.

99. The nature of this action and the nature of laws available to Plaintiff and Subclass Members make use of the class action device, a particularly efficient and appropriate procedure to afford relief to Plaintiff and Subclass Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since it would be able to exploit and overwhelm the limited resources of each individual Subclass Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Subclass and will establish the right of each Subclass Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

100. The litigation of the Subclass claims brought herein is manageable. Defendant's uniform conduct, the relevant laws' consistent provisions, and the Class Members' ascertainable identities demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

101. Adequate notice can be given to Class and Subclass Members directly using information maintained in Defendant's records.

102. Unless a Class and Subclass-wide injunction is issued, Defendant may continue in its failure to secure the PII of Class and Subclass Members properly, Defendant may continue to refuse to provide proper notification to Class and Subclass Members regarding the Data Breach, and Defendant may continue to act unlawfully as outlined in this complaint.

103. Further, Defendant has acted or refused to act on grounds generally applicable to the Class and Subclass and, accordingly, final injunctive or corresponding declaratory relief with

regard to the Class and Subclass Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

104. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiff and members of the Class and Subclass to exercise due care in collecting, storing, using, and safeguarding their PII;

b. Whether Defendant breached a legal duty to Plaintiff and members of the Class and Subclass to exercise due care in collecting, storing, using, and safeguarding their PII;

c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether an implied contract existed between Defendant on the one hand, and Plaintiff and members of the Class and Subclass on the other, and the terms of that implied contract;

e. Whether Defendant breached the implied contract;

f. Whether Defendant adequately and accurately informed Plaintiff and members of the Class and Subclass that their PII had been compromised;

g. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

h. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiff and Class Members; and,

i. Whether Class and Subclass Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Subclass)

105. Plaintiff realleges and incorporates by reference all preceding factual allegations as if fully set forth herein.

106. Plaintiff brings this Count on his own behalf and behalf of the Nationwide Subclass.

107. As a condition of being past and current customers of Defendant, Plaintiff and members of the Subclass were obligated to provide and entrust Defendant with certain PII.

108. Plaintiff and members of the Subclass provided and entrusted their PII to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their PII for business purposes only, and not disclose their PII to unauthorized third parties.

109. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and the Subclass could and would suffer if the PII were wrongfully disclosed.

110. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII of Plaintiff and the Subclass involved an unreasonable risk of harm to Plaintiff and the Subclass, even if the harm occurred through the criminal acts of a third party.

111. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that the PII of Plaintiff and the Subclass in Defendant's possession were adequately secured and protected.

112. Defendant also had a duty to exercise appropriate clearinghouse practices to remove from an Internet-accessible environment the PII it was no longer required to retain pursuant to

regulations and had no reasonable need to maintain in an Internet-accessible climate.

113. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of the PII of Plaintiff and the Subclass.

114. Defendant also had a duty to protect against the reasonably foreseeable criminal conduct of a third party as it was on notice that the failure to protect the PII that it collected for its own pecuniary benefit would harm the Plaintiff and the Subclass.

115. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and the Subclass. That special relationship arose because Plaintiff and the Subclass entrusted Defendant with their confidential PII, a necessary part of obtaining services from Defendant.

116. Defendant was and is subject to an "independent duty," untethered to any contract between Defendant and Plaintiff or the Class and Subclass.

117. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Subclass was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

118. Plaintiff and the Subclass were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the PII of Plaintiff and the Subclass, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on Defendant's systems.

119. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and the Subclass. Defendant's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included

its decisions not to comply with industry standards for the safekeeping of the PII of Plaintiff and the Subclass, including basic encryption techniques freely available to Defendant.

120. Plaintiff and the Subclass had no ability to protect their PII that was in, and possibly remains in, Defendant's possession.

121. Defendant was in an exclusive position to protect against the harm suffered by Plaintiff and the Subclass as a result of the Data Breach.

122. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII of Plaintiff and the Subclass.

123. Defendant has admitted that the PII of Plaintiff and the Subclass were wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

124. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and the Subclass by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII of Plaintiff and the Subclass when the PII was within Defendant's possession or control.

125. Defendant improperly and inadequately safeguarded the PII of Plaintiff and the Subclass in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

126. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect the PII of Plaintiff, the Class, and the Subclass in the face of increased risk of theft.

127. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and the Subclass by failing to have appropriate procedures in place to detect and prevent dissemination of the PII.

128. Defendant breached its duty to exercise appropriate clearinghouse practices by failing to remove from the Internet-accessible environment any PII it was no longer required to retain pursuant to regulations and that Defendant had no reasonable need to maintain in an Internet-accessible environment.

129. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiff and the Subclass the existence and scope of the Data Breach.

130. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Subclass, the PII of Plaintiff and the Subclass would not have been compromised.

131. There is a close causal connection between Defendant's failure to implement security measures to protect the PII of Plaintiff and the Subclass and the harm, or risk of imminent harm, suffered by Plaintiff, the Class, and the Subclass. The PII of Plaintiff and the Nationwide Class was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

132. As a direct and proximate result of Defendant's negligence, Plaintiff and the Subclass have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how its PII is used; (iii) the compromise, publication, and/or theft of its PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of its PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated

with placing freezes on credit reports; (vii) the continued risk to its PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect the PII of Plaintiff and the Subclass; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Subclass.

133. As a direct and proximate result of Defendant's negligence, Plaintiff and the Subclass have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

134. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff, and the Subclass have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

135. As a direct and proximate result of Defendant's negligence, Plaintiff and the Subclass are entitled to recover actual, consequential, and nominal damages.

COUNT II
Negligence Per Se
(On Behalf of Plaintiff and the Subclass)

136. Plaintiff realleges and incorporates by reference all preceding factual allegations as if fully set forth herein.

137. Plaintiff brings this Count on his own behalf and on behalf of the Subclass.

138. "Section 5 of the FTC Act [15 U.S.C. § 45] is a statute that creates enforceable

duties, and this duty is ascertainable as it relates to data breach cases based on the text of the statute and a body of precedent interpreting the statute and applying it to the data breach context." *In re Capital One Consumer Data Sec. Breach Litig.*, 488 F. Supp. 3d 374, 407 (E.D. Va. 2020). "For example, in *F.T.C. v. Wyndham Worldwide Corp.*, 799 F.3d 236, 240 (3d Cir. 2015), the United States Court of Appeals for the Third Circuit affirmed the FTC's enforcement of Section 5 of the FTC Act in data breach cases." *Capital One Data Security Breach Litigation*, 488 F. Supp. 3d at 407.

139. Plaintiff and the Subclass members are in the group of persons the FTC Act was enacted and implemented to protect, and the harms they suffered in the Data Breach as a result of Defendant's violations of the FTC Act were the types of harm they were designed to prevent.

140. As a result of the conduct of Defendant that violated the FTC Act, Plaintiff and the Subclass members have suffered and will continue to suffer foreseeable harm. Plaintiff and the Subclass members have suffered actual damages including, but not limited to, imminent risk of identity theft; expenses and/or time spent on credit monitoring for a period of years; scrutinizing bank statements, credit card statements, and credit reports; time spent initiating fraud alerts and credit freezes and subsequently temporarily lifting credit freezes; and increased risk of future harm. Further, Plaintiff and the Subclass have suffered and will continue to suffer other forms of injury and/or harm including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

COUNT III
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Subclass)

141. Plaintiff realleges and incorporates by reference all preceding factual allegations as if fully set forth herein.

142. Plaintiff brings this Count on his own behalf and on behalf of the Subclass.

143. When Plaintiff and Subclass members provided their PII in exchange for online betting and/or igaming services they entered into implied contracts[23] in which Defendant agreed to comply with its statutory and common law duties to protect the PII of Plaintiff and the Subclass Members and to timely notify them in the event of a data breach.

144. Defendant required Plaintiff and Subclass Members to provide their PII in order for them to use Defendant's services. Plaintiff and the Subclass entrusted their PII to Defendant. In so doing, Plaintiff and the Subclass entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such PII, keep such PII secure and confidential, and timely and accurately notify Plaintiff and the Subclass if their PII had been compromised or stolen.

145. Plaintiff and Subclass members would not have provided their PII to Defendant had they known that Defendant would not safeguard their PII, as promised, or provide timely notice of the Data Breach.

146. Plaintiff and Subclass members fully performed their obligations under implied contracts with Defendant.

147. Defendant breached the implied contracts by failing to safeguard Plaintiff's and Subclass's PII and by failing to provide them with timely and accurate notice of the Data Breach.

148. Defendant's conduct and statements confirm that Defendant intended to bind itself to protect the PII that Plaintiff and the Subclass entrusted to Defendant.

149. Plaintiff and the Subclass fully performed their obligations under the implied contracts with Defendant.

[23] There was an implied contract between Plaintiff and Borgata, and BetMGM succeeded to the rights and obligations under that contract by virtue of its acquisition of Borgata's online betting business.

150. Defendant breached the implied contracts it made with Plaintiff and the Subclass by (i) failing to use commercially reasonable physical, managerial, and technical safeguards to preserve the integrity and security of Plaintiff's and the Subclass's PII, (ii) failing to encrypt social security numbers and sensitive PII, (iii) failing to delete PII it no longer had a reasonable need to maintain, and (iv) otherwise failing to safeguard and protect their PII and by failing to provide timely and accurate notice to them that PII was compromised as a result of the data breach.

151. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Subclass have suffered (and will continue to suffer) the threat of the sharing and detrimental use of their sensitive information; ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

152. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Subclass are entitled to recover actual, consequential, and nominal damages.

COUNT IV
Declaratory Judgment
(On Behalf of Plaintiff and the Nationwide Class)

153. Plaintiff realleges and incorporates by reference all preceding factual allegations as if fully set forth herein.

154. Plaintiff brings this Count on his own behalf and on behalf of the Nationwide Class.

155. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant the further necessary relief. Further, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this complaint.

156. An actual controversy has arisen after the Data Breach regarding Plaintiff's and the Nationwide Class's PII and whether Defendant is currently maintaining data security measures adequate to protect Plaintiff and the Nationwide Class from further data breaches that compromise their PII. Plaintiff and the Nationwide Class allege that Defendant's data security measures remain inadequate. Defendant publicly denies these allegations. Furthermore, Plaintiff and the Nationwide Class continue to suffer injury due to the compromise of their PII. Plaintiff and the Nationwide Class remain at imminent risk that further compromises of their PII will occur. It is unknown what specific measures and changes Defendant has undertaken in response to the Data Breach.

157. Plaintiff and the Nationwide Class have an ongoing, actionable dispute arising out of Defendant's inadequate security measures, including (i) Defendant's failure to encrypt Plaintiff' and the Nationwide Class's PII, including social security numbers while storing it in an Internet-accessible environment and (ii) Defendant's failure to delete PII it has no reasonable need to maintain in an Internet-accessible environment, including the driver's license number of Plaintiff.

158. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owes a legal duty to secure the PII of past and current customers of Defendant;

b. Defendant continues to breach this legal duty by failing to employ reasonable measures to secure consumers' PII; and

c. Defendant's ongoing breaches of its legal duty continue to cause Plaintiff and the Nationwide Class harm.

159. This Court should also issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with law, industry, and government regulatory standards to protect consumers' PII. Specifically, this injunction should, among other things, direct Defendant to:

a. Engage third party auditors, consistent with industry standards, to test its systems for weakness and upgrade any such weakness found;

b. Audit, test, and train its data security personnel regarding any new or modified procedures and how to respond to a data breach;

c. Regularly test its systems for security vulnerabilities, consistent with industry standards; and

d. Implement an education and training program for appropriate employees regarding cybersecurity.

160. If an injunction is not issued, Plaintiff and the Nationwide Class will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Defendant. The risk of another such breach is real, immediate, and substantial. If another breach of Defendant's databases occurs, Plaintiff and the Nationwide Class will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

161. The hardship to Plaintiff and the Nationwide Class if an injunction is not issued exceeds the hardship to Defendant if an injunction is issued. Plaintiff and the Nationwide Class will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to use such measures.

162. Issuance of the requested injunction will satisfy the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Defendant, thus eliminating the additional injuries that would result to Plaintiff, the Nationwide Class, and others whose confidential information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE Plaintiff Scott Madlinger, individually and on behalf of the Class (Count Four), requests that the Court:

A. Certify this case as a class action on behalf of the Class defined above pursuant to Rule 23(b)(2), appoint Plaintiff as the Class representative, and appoint the undersigned counsel as Class counsel;

B. Award declaratory, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class members;

C. Award injunctive relief requiring Defendant to provide an accounting identifying all members of the class and subclass;

D. Enter a declaratory judgment that Defendant committed negligence and negligence per se and that Defendant breached its implied contract with Plaintiff and the Class;

E. Award injunctive relief enjoining Defendant from engaging in future negligence, negligence per se, and breaches of contract;

F. Award injunctive relief requiring Defendant to provide notice to all members of the class that its data breach constituted negligence, negligence per se, and a breach of its implied contracts with the Class, and that if they were harmed that they can bring individual actions for common law relief for damages under negligence, negligence per se, and breach of implied contract claims; and

G. Award such other and further relief as equity and justice may require.

WHEREFORE Plaintiff Scott Madlinger, individually and on behalf of the Subclass (Counts One, Two, and Three), requests that the Court:

A. Certify this case as a class action on behalf of the Subclass defined above pursuant to Rule 23(b)(3), appoint Plaintiff as the Subclass representative,

and appoint the undersigned counsel as Subclass counsel;

B. Award restitution and damages to Plaintiff and Subclass members in an amount to be determined at trial;

C. Award Plaintiff and Subclass members their reasonable litigation expenses and attorneys' fees to the extent allowed by law;

D. Award Plaintiff and Subclass members pre- and post-judgment interest, to the extent allowable; and

E. Award such other and further relief as equity and justice may require.

DEMAND FOR JURY TRIAL

Plaintiff Scott Madlinger, individually and on behalf of the putative Class and Subclass, demands a trial by jury of any and all issues in this action so triable of right.

Respectfully submitted,

/s/ Javier L. Merino
Javier L. Merino, Esq. (078112014)
1520 U. S. Highway 130, Suite 101
North Brunswick, NJ 08902
Telephone: (732) 545-7900
Facsimile: (216) 373-0536
notices@dannlaw.com

Marc E. Dann (OH #0039425)
Brian D. Flick (OH #0081605)
DannLaw
15000 Madison Avenue
Lakewood, OH 44107
Telephone: (216) 373-0539
Email: *notices@dannlaw.com*

/s/ Kevin Laukaitis
Kevin Laukaitis
LAUKAITIS LAW FIRM LLC
737 Bainbridge Street #155
Philadelphia, PA 19147
Phone: 215-789-4462
Email: klaukaitis@laukaitislaw.com

/s/ James. E Cecchi
James E. Cecchi
Lindsey H. Taylor
CARELLA, BYRNE, CECCHI, OLSTEIN, BRODY & AGNELLO, P.C.
5 Becker Farm Road
Roseland, New Jersey 07068
(973) 994-1700
jcecchi@carellabyrne.com

/s/ Courtney E. Maccarone
Courtney E. Maccarone
Mark S. Reich
LEVI & KORSINSKY, LLP
55 Broadway
4th Floor, Suite #427
New York, NY 10006
(212) 363-7500

/s/ Andrew Jimin Heo
Andrew Jimin Heo
Jeffrey W. Golan
BARRACK, RODOS & BACINE
3300 Two Commerce Square
2001 Market Street
Philadelphia, PA 19103
215-963-0600
aheo@barrack.com
jgolan@barrack.com

Counsel for Plaintiff Scott Madlinger and the Putative Class and Putative Subclass